Forensics Role and Framework

Table of Contents

Mobile Device Incident Response -1 ................................................................. 2
Mobile Device Incident Response -2 ................................................................. 7
Mobile Device Incident Response -3 ................................................................. 10
Mobile Forensics Process Framework ............................................................. 12
Notices ............................................................................................................... 14
Mobile Device Incident Response

Proper handling of mobile devices on-scene is vital. Safety and evidence preservation are critical; each individual must know and understand his/her role and responsibility.

On-scene roles and responsibilities:

- CIRT Team Leader / Lead Investigator
- Photographer and Sketcher
- Technical Lead / Specialist
- Evidence Recorder / Custodian

If I'm a police officer working on a crime scene, and later down the road the defense can prove that I somehow mishandled the devices that were on scene, or I didn't do a procedural step that I needed to take, like a chain of custody.

Regardless of what I find four steps down in the process-- so I've done- I've used the Cellebrite tool, I've done the analysis, and during the analysis I found the email that said: "I'm going to rob the bank."
If I don’t do the correct procedural steps up front-- if I don’t collect the evidence correctly; if I don’t fill out the proper forms-- that evidence might never reach the jury. The defense attorney can get it thrown out of court before what I found in Step 4 is ever presented to the jury.

So the crime scene- the on-scene stuff itself is extremely vital when we talk about cell phone, or any type of computer forensics.

The first-- safety is always paramount. Officer safety is always the first thing that needs to be kept in mind when we’re talking about a criminal on-scene investigation.

I don’t care if you think systems are being wiped. I don’t think if somebody called and told you, ”I can see the systems being wiped as we speak.” You always make sure the safety of the officer is taken care of.

If somebody's on-scene with a gun, you don't have somebody go run after the computers while that person still has the weapon. You get the weapon out of the person's hands, and then you worry about the rest; even if during the timeframe something got lost-- either wiped or destroyed, etcetera.

You never compromise officer safety. I don’t care how important the case is.

Plus each person on-scene needs to understand their role. So on-scene
roles and responsibility-- and there can be more than one person filling some of these roles. Some roles you’re better off with one person.

Such as the CIRT team leader/lead investigator. This should be-- for this crime scene, you should have one person identified as the team leader. That’s the person that makes the determination which evidence are we going to collect first?

And of course, those questions should be based on past experience. So you want somebody that’s very experienced in handling crime scenes as the team leader. It doesn’t necessarily need to be a forensic person.

You have the forensic people in the other roles. They know what they need to do. The team leader should just be very, very understand-- not understanding. They have to know how to handle a crime scene. And that comes with years of experience.

A lot of computer crime people don’t necessarily go on-scene. A lot of times they’re back in the lab. The regular officers collect the stuff on-scene and send it to the lab for analysis.

So the person that’s in lead has to have a general understanding; but they don’t have to be an expert on computer or cell phone forensics. They just have to control the scene. If there’s any questions, they either need to be able to answer those
questions, or point people to who can answer those questions, or find out the answers.

The photographer and the sketcher. Before devices are collected, pictures should be taken of where they are. Pictures should be taken of the devices themselves. Can you see fingerprints on the screen? Somebody should take a picture of that screen.

Are there SIM cards outside of a phone just-- let’s say there’s a SIM card sitting next to a cell phone. You might want to document that in a picture.

You want to be able to say: "This phone was found in this room, at this location." You want to be able to be that specific when you’re talking about-- later on when you’re having to testify on the information.

The photographer and the sketcher-- and you might have just one, you might have both; depends on the scene-- should be able to allow you, when you’re on the stand later, to remember: "Oh yes, that cell phone was found next to the body that was on the ground."

The technical lead/specialist. This should be somebody, if possible, that is an expert in whatever’s being collected; whether it’s-- if computers are being collected, it should be a computer forensic expert. If it’s a cell phone, it should be a cell phone forensic expert. This is the person that any technical questions will go to.
And then evidence recorder/custodian. There should be one person responsible for collecting all evidence on the scene. You don’t want multiple people collecting evidence, if at all possible.

If multiple people are collecting evidence, they should all— all the evidence should be taken to the evidence recorder. They will sign the evidence in and become responsible for the evidence until it reaches the— wherever you’re going.

And this is more true for criminal investigations than it would be for an organization.

If I’m HP- if I work for HP, even though some of the same principles apply— you’re going to fire somebody and you need to make sure you get all the phones that that person has before he’s fired. I’m not going to have the same roles. But a lot of the same principles apply.

I’m going to have— any phones he gives me, I’m going to make him sign an Evidence Form 4. That way he shows that he turned them in— so that protects him— and we have his signature that he turned them in; so that protects us. So at a later date and time he can’t come back and say: “They took my personal phone.”

Well here’s the forms we filled out and he signed; and you can see he gave us X, Y, Z items. And these are the only items that he gave us.
So it's not a direct one-to-one between crime scenes and an organization in how you would handle it; but some of the same principles apply when we're talking about how did we get the evidence from a location.

**Mobile Device Incident Response -2**

**Mobile Device Incident Response -2**

CIRT Team Leader / Lead Investigator is responsible for evaluating the scene, ensuring team members are trained and well-equipped, and guiding the actions of the team members.

A mobile device can be used as a detonator for improvised explosive devices (IED). Caution and awareness must be adhered prior to handling a mobile device in an unknown environment.

Technical Lead / Specialist, when authorized by the Lead Investigator/Team Lead, ensures the mobile devices and digital evidence is collected in a forensically sound manner to protect and preserve the evidence.

This should not be going on as you arrive on the scene. You should already have these roles identified; hopefully weeks in advance. Hopefully as you do more and more crime scenes, the same people fill the same roles.
And they ultimately guide the actions of the team members. If there's any questions, ultimately it's the team leader's responsibility to handle whatever comes up while on-scene.

As an FYI: Mobile devices-- and this doesn't happen often; this would be more something you would see in a theater of war location-- mobile devices can be used as a detonator for IEDs.

You see this a lot in the Middle East-- Afghanistan, Iraq-- where there's a device on the side of the road. Somebody calls that device at a certain time when a convoy is going past it and it explodes.

We haven't really seen it much in the U.S. It can occur though.

So if you're in a- and if you're in a- on a scene where you think this type of violence might occur, team members must be cautious and aware that this capability exists. Excuse me.

The Technical Lead/Specialist. When authorized by the lead investigator, they ensure that mobile devices and digital evidence is collected in a forensically sound manner.

So one of the things you have to worry about when collecting evidence, or cellular evidence, is: Is this device still talking to the cellular network? Because if it is-- or a Wi-Fi network for that matter-- if this
device is, most mobile devices allow the ability to remote wipe, either by the user or by the carrier.

So if I come on-scene and there's--let's just say these pens are cell phones--and there's two cell phones located over here. I can't just say: "Oh, I'm going to collect this cell phone. I'm going to put it in a normal bag and I'm going to take it back to the office and then handle everything there."

Because on the way back to the office, however long it takes to get there, the data might be being wiped. So I have a perfectly good cellular device while on-scene. By the time I get back I have a brick that doesn't have any investigative purposes whatsoever.

So as the technical lead, I have to make the determination how am I going to prevent these devices from talking to the network? And that's--there's a couple of different solutions we can discuss to help that. But the technical lead is ultimately responsible for that type of information.

The CIRT team leader might not have any background in cellular forensics. They might not know that these devices can be remotely wiped. It is up to the technical lead to ensure that the team leader understands special handling instructions for devices.
The same is true if they came across a server with a RAID. The technical lead for the computer side needs to make the call on how exactly they're going to get that server back to the Police Department for analysis. Do we just pull the plug? Do we do a graceful shutdown? Do we just take the drives? Falls on the technical lead to make that call.

**Mobile Device Incident Response -3**

**Photographer and Sketcher** ensures everything is photographed and documented before being collected.

**Evidence Recorder / Custodian** coordinates with the photographer and specialist to ensure evidence is documented and stored properly.

**009 The photographer and sketcher may be the same person; may be two people; could be five people taking photographs and sketching the scene. Don't necessarily need both. Maybe you just have a photographer. Maybe you just have a sketcher.**
I've seen more scenes that just have a photographer than have just a sketcher.

If you have both, great. It’s easier to identify exactly where something was found when you have both photos and a sketch that shows where items were located.

The Evidence Recorder. Coordinates with the photographer and the specialist to ensure evidence is documented and stored properly.

So they’re not going to start collecting evidence until pictures of those devices, wherever they’re located, have been taken. They’re going to be the first person on the chain of custody; if they’re doing the entire collection.

If multiple people are collecting and bringing it to the evidence recorder, the person that originally collects it will sign it over to the evidence recorder.

You don’t-- I haven’t seen an instance where I would want more than one evidence recorder. I could see potentially a crime scene that has thousands of computers; maybe then you have one evidence recorder per room.

But in most cases you’re not going to have that many pieces of evidence; and you want one person to know all of the evidence for an area. Otherwise, you get into the situation where: Oh I thought you collected
Mobile Forensics Process Framework

Because of the dynamic nature of a smartphone, understanding and having a forensic process in place is crucial to properly preserving and analyzing the data contained in the mobile device.

1. Identification
2. Preservation
3. Acquisition
4. Analysis
5. Archiving
6. Reporting

**So here is the Mobile Forensics Process Framework. Because of the dynamic nature of smartphones, there has to be a process in place to properly preserve and analyze the data contained in the mobile device.**

Anybody that does any one of these steps need to understand how they fit into this framework; and why this framework is important.
This framework provides the repeatable process that ensures by the time the evidence eventually ends up in court-- which can be a year or two down the road sometimes; it can be a long time-- that when it gets to court you can prove that from the very first step of identifying the evidence that we followed our process; the process we follow every time.

And we ensured that the evidence was maintained in an acceptable manner. We used sound forensic tools. Here's how we analyzed the findings. Here's how we stored the evidence, so that it didn't change. And here's the report we generated.

Because after the report-- again, it could be months or years before that evidence ever reaches the court. And will you remember exactly what steps you took, if you're not following a process framework?

It's not good to be on the stand and be like, "We didn't really have a process for this. I'm not quite sure what we did in this-- I know we used our forensic tool, but I can't tell you exactly when we did it or anything else."

Because the judge is going to look at you and be like, "I can't accept your testimony in this case."
Copyright 2013 Carnegie Mellon University

This material has been approved for public release and unlimited distribution except as restricted below. This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study. Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The U.S. Government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

NO WARRANTY. THE MATERIAL IS PROVIDED ON AN 'AS IS' BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark of Carnegie Mellon University.